

UNITED STATES DISTRICT COURT

for the
Western District of Washington

FILED	LODGED
RECEIVED	
Jan 24 2023	
CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT TACOMA	
BY	DEPUTY

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Information stored by Google

Case No. 3:23-mj-05023

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is incorporated herein by reference
located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

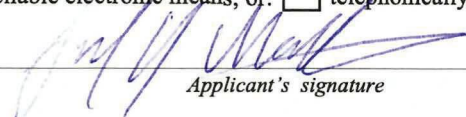
Code Section	Offense Description
18 U.S.C. 1366	Damage to Energy Facility
18 USC 371	Conspiracy

The application is based on these facts:

- ☒ See Affidavit of Special Agent Samuel Wharton continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.



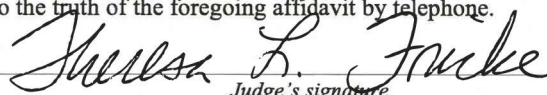
Applicant's signature

Samuel Wharton, Special Agent, FBI

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 01/24/2023



Judge's signature

City and state: Seattle, Washington

Theresa Fricke, United States Magistrate Judge

Printed name and title

ATTACHMENT A

Description of Information to be Searched

Identifying information for the following four SUBJECT DEVICES (Google Accounts),
pertaining to the case with Google Reference Number 28285386:

Location 3 (200 North Pekin Road Woodland, Washington)

- (1) 010101BD56354D7944778340B2CFEE63ABD6A2076E8178D5B0A8CC8EBC1
ABEBFE39DBF2EF96C37

For the following time period in Pacific Standard Time:

4:00 a.m. through 5:00 a.m. (PST) on November 18, 2022.

Location 7 (8396 SE Sunnyside Road Clackamas, Oregon)

- (2) 010101BD56354D5F5CEB3026ACBDA34AD51CCD61EFD87C8455B5FFFB7
CEBC8C07C4AAAB992A725
- (3) 010101BD56354DAAC9695949E1D6BBB4DE8A8FCF409F99F650A0A0392A
D02F0FBCB8ABB689CD91
- (4) 010101BD56354DCAF9370765033E319FBF69546D901796446D94EB41E7646
856757DEB2CBFA444

For the following time period in Pacific Standard Time:

12:30 a.m. to 1:10 a.m. (PST) on November 28, 2022.

ATTACHMENT B

Information to be Searched for and Seized

All the information associated with the SUBJECT DEVICES as described in Attachment A that constitutes evidence of violations Title 18, United States Code, Section 1366 (Destruction of Energy Facilities).

GOOGLE shall produce, for the SUBJECT DEVICES, the following:

The identifying subscriber information associated with the SUBJECT DEVICES and any associated Google accounts or services, including the International Mobile Equipment Identifier (IMEI), International Mobile Subscriber Identity (IMSI), internet protocol addresses, telephone numbers, mobile carrier codes, and e-mail addresses.

Google is hereby ordered to disclose the above information to the government within fourteen (14) days of service of these warrants.

AFFIDAVIT OF SAMUEL WHARTON

STATE OF WASHINGTON)
)
) SS.
COUNTY OF THURSTON)

I, Samuel Wharton, a Special Agent with the Federal Bureau of Investigation, being duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since September 2017. My current assignment is with the FBI Seattle Field Office, South Sound Joint Terrorism Task Force, investigating a variety of criminal and national security matters, including violent crimes and major offenses such as threats to human life, threats to damage property, actual and attempted bombings, and efforts to use violence in support of, or to counter, a particular ideology. My training and experience include a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause. As an FBI agent, I have investigated several criminal violations, including narcotics trafficking, homicide, and international and domestic terrorism. I have also served as the affiant for search warrants, including search warrants for electronic evidence.

The facts set forth in this Affidavit are based on my personal knowledge; knowledge obtained from other individuals during this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for search warrants, it does not set forth every fact that I, or others, have learned during this investigation.

//

//

RELEVANT STATUTE

Title 18, United States Code, Section 1366 defines offenses for causing destruction to an “energy facility.” Section (a) of the statute makes it a felony offense where one “knowingly and willfully damages or attempts or conspires to damage the property of an energy facility in an amount that in fact exceeds or would if the attempted offense had been completed, or if the object of the conspiracy had been achieved, have exceeded \$100,000, or damages or attempts or conspires to damage the property of an energy facility in any amount and causes or attempts or conspires to cause a significant interruption or impairment of a function of an energy facility.” Section (b) defines a lesser-included felony offense where one “knowingly and willfully damages or attempts to damage the property of an energy facility in an amount that in fact exceeds or would if the attempted offense had been completed have exceeded \$5,000.” The term “energy facility” is defined as “a facility that is involved in the production, storage, transmission, or distribution of electricity, fuel, or another form or source of energy, or research, development, or demonstration facilities relating thereto . . .” 18 U.S.C. § 1366(c).

**BACKGROUND RELATING TO GOOGLE’S SERVICES
AND RELEVANT TECHNOLOGY**

Based on my training and experience, I know that cellular devices, such as mobile telephones, are wireless devices that enable their users to send and receive wire and/or electronic communications using the networks provided by cellular service providers. In order to send or receive communications, cellular devices connect to radio antennas that are part of the cellular network called “cell sites,” which can be mounted on towers, buildings, or other infrastructure. Cell sites provide service to specific geographic areas, although the service area of a given cell site will depend on factors including the distance between towers. As a result, information about what cell site a cellular device connected to at a specific time can provide the basis for an inference about the general geographic location of the device at that point.

1 I also know that many cellular devices such as mobile telephones have the capability
2 to connect to wireless internet (“wi-fi”) access points if a user enables wi-fi connectivity.
3 Wi-fi access points, such as those created using a router and offered in places such as homes,
4 hotels, airports, and coffee shops, are identified by a service set identifier (“SSID”) that
5 functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely
6 scan their environment to determine what wi-fi access points are within range and will
7 display the names of networks within range under the device’s wi-fi settings.

8 Based on my training and experience, I also know that many cellular devices feature
9 Bluetooth functionality. Bluetooth allows for short-range wireless connections between
10 devices, such as between a mobile device and Bluetooth-enabled headphones. Bluetooth uses
11 radio waves to allow the devices to exchange information. When Bluetooth is enabled, a
12 mobile device routinely scans its environment to identify Bluetooth devices, which emit
13 beacons that can be detected by mobile devices within the Bluetooth device’s transmission
14 range, to which it might connect.

15 I also know that many cellular devices, such as mobile telephones, include global
16 positioning system (“GPS”) technology. Using this technology, the phone can determine its
17 precise geographical coordinates. If permitted by the user, this information is often used by
18 apps installed on a device as part of the app’s operation.

19 Based on my training and experience, I know Google is a company that, among other
20 things, offers an operating system (“OS”) for mobile devices, including cellular phones,
21 known as Android. Nearly every cellular phone using the Android operating system has an
22 associated Google account, and users are prompted to add a Google account when they first
23 turn on a new Android device.

24 In addition, based on my training and experience, I know that Google offers numerous
25 apps and online-based services, including messaging and calling (*e.g.*, Gmail, Hangouts,
26 Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage,
27 and sharing (*e.g.*, Drive, Keep, Photos, and YouTube). Many of these services are accessible
28 only to users who have signed into their Google accounts. An individual can obtain a Google

1 account by registering with Google, and the account identifier typically is in the form of a
2 Gmail address (*e.g.*, example@gmail.com). Other services, such as Maps and YouTube, can
3 be used with limited functionality without the user being signed into a Google account.

4 Based on my training and experience, I also know Google offers an Internet browser
5 known as Chrome that can be used on both computers and mobile devices. A user can sign-
6 in to a Google account while using Chrome, which allows the user's bookmarks, browsing
7 history, and other settings to be uploaded to Google and then synced across the various
8 devices on which the subscriber may use the Chrome browsing software, although Chrome
9 can also be used without signing into a Google account. Chrome is not limited to mobile
10 devices running the Android operating system and can also be installed and used on Apple
11 devices and Windows computers, among others.

12 Based on my training and experience, I know that, in the context of mobile devices,
13 Google's cloud-based services can be accessed either via the device's Internet browser or via
14 apps offered by Google that have been downloaded onto the device. Google apps exist for,
15 and can be downloaded to, devices that do not run the Android operating system, such as
16 Apple devices.

17 According to my training and experience, as well as open-source materials published
18 by Google, I know that Google offers accountholders a service called "Location History,"
19 which authorizes Google, when certain prerequisites are satisfied, to collect and retain a
20 record of the locations where Google calculated a device to be based on information
21 transmitted to Google by the device. That Location History is stored on Google servers, and
22 it is associated with the Google account that is associated with the device. Each
23 accountholder may view their Location History and may delete all or part of it at any time.

24 Based on my training and experience, I know that the location information collected
25 by Google and stored within an account's Location History is derived from sources including
26 GPS data and information about the wi-fi access points and Bluetooth beacons within range
27 of the device. Google uses this information to calculate the device's estimated latitude and
28 longitude, which varies in its accuracy depending on the source of the data. Google records

1 the margin of error for its calculation as to the location of a device as a meter radius, referred
2 to by Google as a “maps display radius,” for each latitude and longitude point.

3 Based on open-source materials published by Google and my training and experience,
4 I know that Location History is not turned on by default. A Google accountholder must opt-
5 in to Location History and must enable location reporting with respect to each specific
6 device and application on which they use their Google account for that usage to be recorded
7 in Location History. A Google accountholder can also prevent additional Location History
8 records from being created at any time by turning off the Location History setting for their
9 Google account or by disabling location reporting for a particular device or Google
10 application. When Location History is enabled, however, Google collects and retains
11 location data for each device with Location Services enabled, associates it with the relevant
12 Google account, and then uses this information for various purposes, including to tailor
13 search results based on the user’s location, to determine the user’s location when Google
14 Maps is used, and to provide location-based advertising. As noted above, the Google
15 accountholder also can view and, if desired, delete some or all Location History entries at
16 any time by logging into their Google account or by enabling auto-deletion of their Location
17 History records older than a set number of months.

18 Location data, such as the location data in the possession of Google in the form of its
19 users’ Location Histories, can assist in a criminal investigation in various ways. As relevant
20 here, I know based on my training and experience that Google can determine, based on
21 location data collected and retained via the use of Google products as described above,
22 devices that were likely in a particular geographic area during a particular time frame and to
23 determine which Google account(s) those devices are associated with. Among other things,
24 this information can indicate that a Google accountholder was near a given location at a time
25 relevant to the criminal investigation by showing that his/her device reported being there.

26 Based on my training and experience, I know that when individuals register with
27 Google for an account, Google asks subscribers to provide certain personal identifying
28 information. Such information can include the subscriber’s full name, physical address,

1 telephone numbers and other identifiers, alternative email addresses, and, for paying
2 subscribers, means and source of payment (including any credit or bank account number). In
3 my training and experience, such information may constitute evidence of the crimes under
4 investigation because the information can be used to identify the account's user or users.
5 Based on my training and my experience, I know that even if subscribers insert false
6 information to conceal their identity, this information often provide clues to their identity,
7 location, or illicit activities.

8 Based on my training and experience, I also know that Google typically retains and
9 can provide certain transactional information about the creation and use of each account on
10 its system. This information can include the date on which the account was created, the
11 length of service, records of login (*i.e.*, session) times and durations, the types of service
12 utilized, the status of the account (including whether the account is inactive or closed), the
13 methods used to connect to the account (such as logging into the account via the provider's
14 website), and other log files that reflect usage of the account. In addition, Google often has
15 records of the Internet Protocol address ("IP address") used to register the account and the IP
16 addresses associated with particular logins to the account. Because every device that
17 connects to the Internet must use an IP address, IP address information can help to identify
18 which computers or other devices were used to access the account.

19 **SUMMARY OF PROBABLE CAUSE**

20 **Extremist Propaganda Calling for Attacks on Energy Facilities**

21 In July 2022, a publication was released online entitled "The Hard Reset." This
22 publication was distributed by groups and individuals that espouse a Racially or Ethnically
23 Motivated Violent Extremist (RMVE) ideology. The publication promotes an ideology
24 known as "accelerationism," which is the idea that society and/or nation states are headed for
25 an inevitable collapse and accelerationists should not wait for the collapse but should take
26 actions to accelerate the collapse. Once this collapse occurs, RMVE groups could then start a
27 race war and establish a white ethnostate.
28

1 The “Hard Reset” publication includes detailed technological specifications
2 regarding different types of critical infrastructure, including water treatment plants, bridges,
3 railways, and energy facilities (such as electric substations), and their vulnerabilities. The
4 publication also provides detailed instructions on how “saboteurs” could best exploit these
5 vulnerabilities to damage or destroy these facilities. The publication advocates for saboteurs
6 to take steps to locate these facilities of critical infrastructure, identify their weak points, and
7 attack them to inflict substantial damage using firearms, arson, and other means.

8 Relevant to this investigation, the “Hard Reset” publication encourages followers to
9 attack energy facilities and, specifically, electrical substations, stating: “Electricity is the
10 main satiating tool the system uses to keep the masses from rioting. ... Without power other
11 types of sabotage become very powerful and harder to repair, as such the impact of a
12 directed outage could exponentially increase the results of a saboteur’s efforts.” Regarding
13 electrical substations, the publication states:

14 Substations are a pillar of the electrical grid, responsible for the distribution,
15 transmission, collection, switching, and conversion depending on the type.
16 Substations are publicly indexed and generally easy to find with any map
17 service. Some services will even provide additional information about a
18 substation. Google street view should be utilized. A saboteur should aim for
19 specific targets while shooting at substations. The breaker is one such target,
20 itself being a giant sophisticated fuse for dealing with large amounts of voltage
21 when things go wrong elsewhere in the power grid. They result on filling a
22 chamber with a non-conductive oil or gas in order to cut current off. They
23 won’t be able to function without their oil. And can catch fire...aim for
24 damage to result not from electrical fires or faulting, but from overheating and
25 oil fires. Radiators and cooling fans, pictured below, should also be targeted.
26 Other targets include oil pumps, oil conservator tank, and electronic controls.

27 The publication includes detailed photographs of transformers and other electrical
28 equipment, with their component parts labeled.

29 In recent months, there have been multiple incidents during which energy facilities in
30 Southwest Washington and Northwest Oregon have been damaged using firearms, blunt
31 objects, and/or arson. The original warrant application submitted to Judge Creatura in

December 2022 documented six incidents that were part of this investigation. However, based on the responsive geofence data provided by Google, the instant warrant application pertains only to two of the incidents (there was no responsive data available for the other incidents). The facts of those two incidents are summarized below.

Location 3: 200 North Pekin Road Woodland, Washington¹

On November 18, 2022, unknown suspects caused damage to the electric substation located at 200 North Pekin Road, Woodland, Washington 98674. This substation is owned and operated by the Cowlitz Public Utility District and receives its electricity from the Bonneville Power Administration. It is responsible for distributing electricity to the town of Woodland and the surrounding areas.

On November 18, 2022, at approximately 4:30 a.m., unknown individuals forced their way under the barbed wire perimeter fence of the substation. Once inside the yard, the individuals broke a window to gain access to the control house.



Inside the control house, they manually manipulated the breakers that control the flow of electricity. The suspects also used a blunt object to smash the exposed, inner

¹ This was referred to as “Location 2” in the original search warrant application. Google renumbered the locations in its response, and we are now using Google’s location numbers.

workings of the breaker towers, rendering multiple components inoperative and in need of either repair or replacement. This resulted in the interruption of electrical service for approximately 1,700 people and set-off alarms at the Cowlitz Public Utility District headquarters. The Cowlitz Public Utility District estimates that the damage caused by this incident was between \$50,000 and \$60,000.



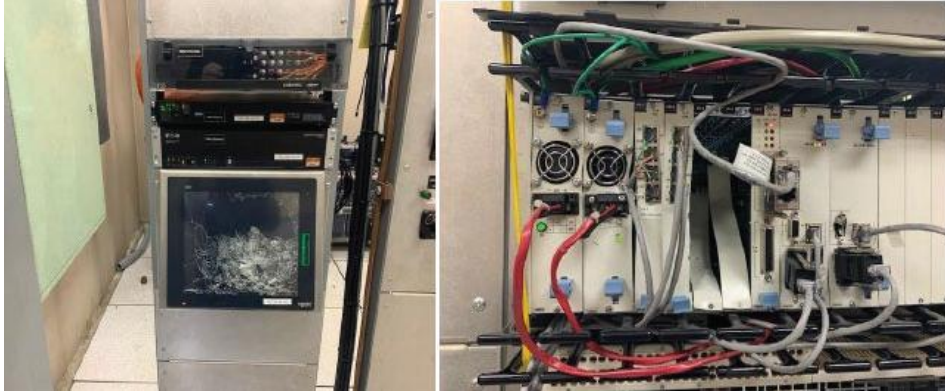
This substation is in a rural area, surrounded by woods and agricultural fields. As such, there are no surveillance cameras in the area. A single, local road runs past the facility, which sees very little traffic during early morning hours.

Location 7: 8396 SE Sunnyside Road Clackamas, Oregon

On November 28, 2022, at approximately 12:49 a.m., unknown suspects caused damage to the electrical substation located at 8396 Southeast Sunnyside Road Clackamas, Oregon. This substation is owned and operated by Portland General Electric. The damage caused by the suspects de-energized the substation's two transmission sources, resulting in a power outage to 6,337 industrial, commercial, and residential customers in the Clackamas area.

During this incident, two unknown suspects cut through a perimeter fence and gained entry to the yard. Once inside the yard, the suspects broke into the control house. Using a blunt object, they smashed the exposed, inner workings of the supervisory control and data

1 acquisition system (“SCADA”), which controls industrial processes such as the gathering of
2 data in real time from remote locations to control equipment and conditions. The attackers
3 also damaged a computer screen and other equipment rendering multiple components
4 inoperative and in need of repair or replacement. According to Portland General Electric, the
5 offense caused a power outage in the surrounding area and damages of approximately
6 \$26,000.



25 The Clackamas County Sherriff’s Office responded to the scene and obtained
26 security camera footage from a nearby business. FBI agents reviewed the video and observed
27 that at approximately 12:37 a.m., at least two unknown suspects entered the camera view
28 wearing dark clothing. They approached the substation’s exterior fence near where it had

1 | been cut open. One of the suspects crouches down by the fence for several minutes. At
2 | approximately 1:02 a.m., one of the suspects appears to climb through the fence and walks
3 | towards the substation control room building, which was ultimately damaged. The video
4 | ends at 1:05 a.m.

5 | This substation is in a populated area with arterial roadways on the north and west
6 | sides. The substation is surrounded by businesses. However, none of the business were open
7 | from midnight to 2:00 a.m. at the time of the attack. The roadways and surrounding area are
8 | active during the day but see little traffic at night while all local businesses are closed.

9 | **Connections Between the Attacks at the Substations**

10 | Based on the FBI's investigation to date, I submit there is probable cause to believe
11 | that the six incidents under investigation are part of a conspiracy to damage electrical
12 | substations in Southwest Washington and Northwest Oregon. There are several reasons to
13 | believe that these incidents are related as part of a conspiracy.

14 | First, the tactics used by the suspects are consistent with the methodologies called for
15 | by the Hard Reset publication. Specifically, the various attacks have used means of firearms,
16 | arson, damaging substation control house equipment, and causing leaks to oil tanks, all of
17 | which are specifically outlined in the Hard Rest. Second, for each of the incidents where
18 | surveillance camera footage is available there appeared to be two suspects who were wearing
19 | dark clothing. These incidents spanned both the Western District of Washington and the
20 | District of Oregon. Third, the means used by the suspects were consistent across certain
21 | incidents. Lastly, BPA employees have told the FBI that the number of attacks in this type of
22 | concentrated period is highly unusual. This suggests that the attacks are part of a coordinated
23 | effort as opposed to random individual events.

24 | **PRIOR SEARCH WARRANT & CURRENT REQUEST**

25 | As noted above, on December 16, 2022, Magistrate Judge J. Richard Creatura issued a
26 | geofence warrant identifying six target locations and time periods relevant to the attacks on
27 | various substations. Among other target locations, the warrant identified the following two
28 | target locations and time periods for which Google was required to provide geolocation data:

Target Location 3:

Geographical box with the following four Google Earth latitude and longitude coordinates near the address of 200 North Pekin Road, Woodland, Washington 98674:



- 1) 45.904174, -122.757840
- 2) 45.904174, -122.756725
- 3) 45.903701, -122.756744
- 4) 45.903707, -122.757540

For the time period of 4:00 a.m. to 5:00 a.m. (PST) on November 18, 2022.

Target Location 7:

Geographical box with the following four Google Earth latitude and longitude coordinates near the address of 8396 SE Sunnyside Road, Clackamas, Oregon 97015:



- 1) 45.432424, -122.579041
- 2) 45.432892, -122.577492
- 3) 45.431571, -122.577249
- 4) 45.431609, -122.579072

For the time period of 12:30 a.m. to 1:10 a.m. (PST) on November 28, 2022.

1 On January 9, 2023, the FBI received data from Google in response to search warrant
2 MJ22-5295, including anonymized lists of devices present at the target locations that fit the
3 time and location parameters set forth above. The devices were referenced by anonymized
4 identifiers that are 78-80 characters long, but for the purposes of simplicity I am referring to
5 them herein only by their last four characters.

6 With respect to **Location 3**, Google provided data showing that one device pinged 20
7 times within the target location at the time of the offense conduct. Investigators analyzed the
8 data provided by Google for this device, including time, latitude/longitude, accuracy in
9 meters, and source of connection. This device, 6C37, pinged with accuracy of between 3 and
10 7 meters a total of 17 times. The latitude/longitude of these pings place this device within the
11 confines of the fenced, substation yard. The location data for this device is consistent with
12 the movements of the unknown individuals who forced their way under the perimeter fence
13 and broke into the control house. It is reasonable to believe that this device is related to the
14 individuals carrying out the attack on the substation. I am therefore seeking additional
15 identifying data for this device.

16 The data provided by Google for **Location 7** showed that three devices pinged a total
17 of 13 times within the target location during the offense conduct. Investigators analyzed the
18 data provided by Google for these devices, including time, latitude/longitude, accuracy in
19 meters, and source of connection. These factors were then compared to information from the
20 video surveillance captured at or around Location 7.

21 According to the Google data, Device A725 pinged within the geofence of Location 7
22 three times, as pictured in *Figure 1* below, with a display radius of 13-18 meters. Therefore,
23
24
25
26
27
28

A725 was present in the vicinity and at the time the suspects completed the attack and is relevant to the investigation.



Figure 1

Device CD91 similarly pinged within Location 7 three times, as pictured in *Figure 2* below, with a display radius of 13-16 meters. Therefore, CD91 was present in the vicinity and at the time the suspects completed the attack and is relevant to the investigation.

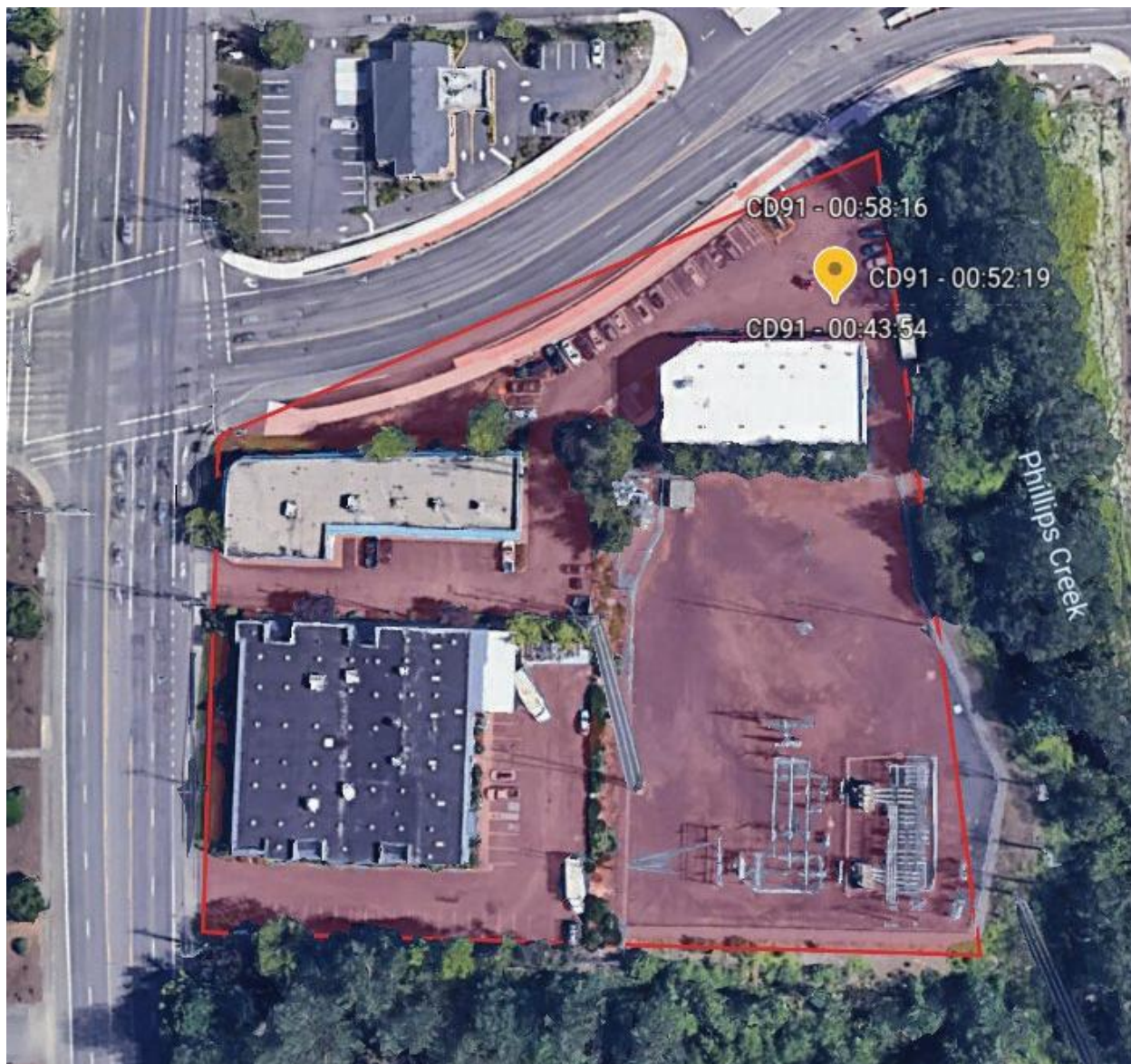


Figure 2

According to the Google data, Device A444 pinged within the geofence of Location 7 seven times, as pictured in *Figure 3* below, with a display radius of 14-116 meters. Therefore, A444 was present in the vicinity and at the time the suspects completed the attack and is relevant to the investigation.

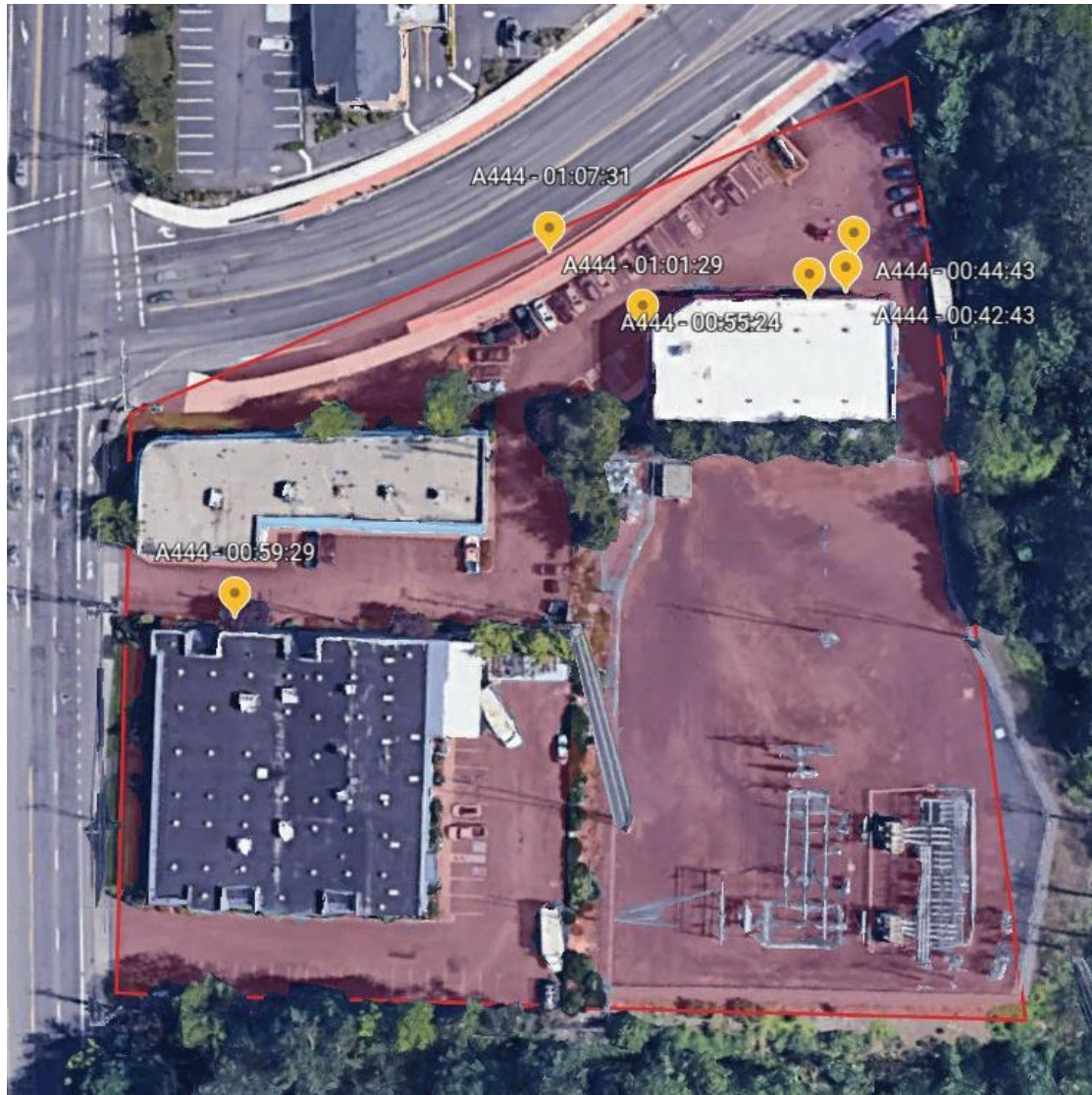


Figure 3

REQUEST FOR SEALING

I further request this Court issue an order sealing all papers submitted in support of the requested search warrants, including the application, this affidavit, the attachments, and the requested search warrants. I believe sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may cause the culpable person(s), or others associated with the culpable person(s) to flee from prosecution, cause destruction of or tampering with evidence,

1 or otherwise seriously jeopardize this investigation. Premature disclosure of the contents of
2 the application, this affidavit, the attachments, and the requested search warrants may
3 adversely affect the integrity of the investigation.

4 **CONCLUSION**

5 Based on the forgoing, I request that the Court issue the proposed warrants, pursuant
6 to pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703.

7 Pursuant to 18 U.S.C. § 2703(g), the government will execute the warrants by serving
8 the warrants on Google. Because the warrants will be served on these providers, who will
9 then compile the requested records and data, reasonable cause exists to permit the execution
10 of the requested warrants at any time in the day or night. I therefore further request that the
11 Court authorize execution of the warrants at any time of day or night. Pursuant to 18 U.S.C.
12 § 2703(g), the presence of a law enforcement officer is not required for the service or
13 execution of these warrants.

1 I declare under penalty of perjury that the statements above are true and correct to the
2 best of my knowledge and belief.

3
4
5 
6 SAMUEL WHARTON
7 Special Agent, FBI

8 The above-named agent provided a sworn statement to the truth of the foregoing
9 affidavit by telephone on the 24th day of January, 2023.

10
11 
12 THERESA FRICKE
13 United States Magistrate Judge
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28